



*Embassy of the United States of America*

Office of Legal Attache  
Bucharest, Romania

File No.

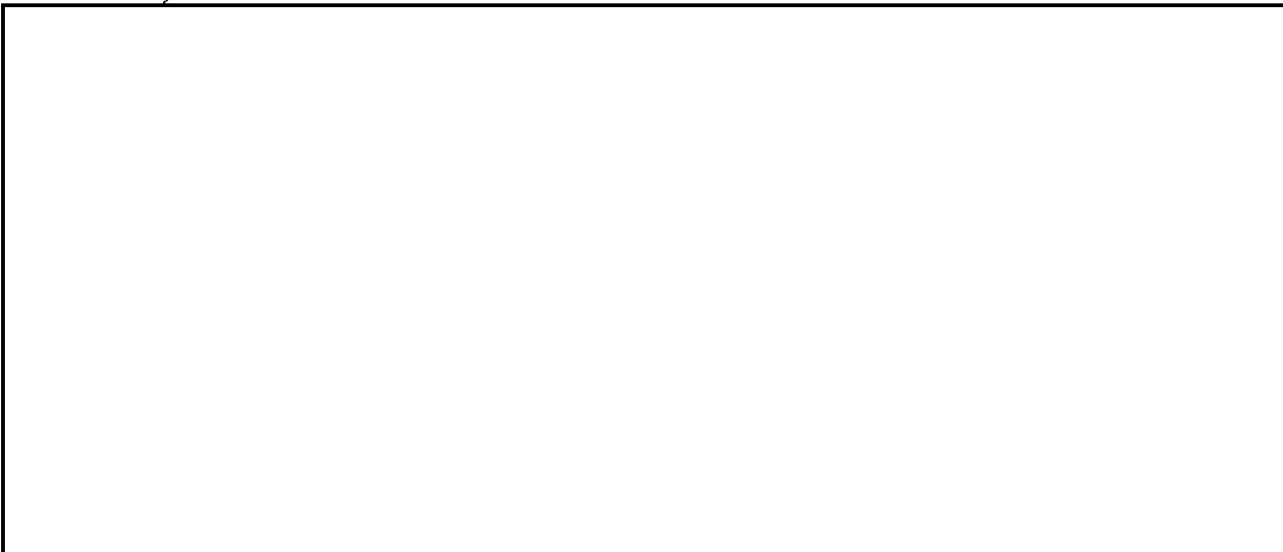
12 April 2012

Romanian Intelligence Service (SRI)  
Bucharest, Romania

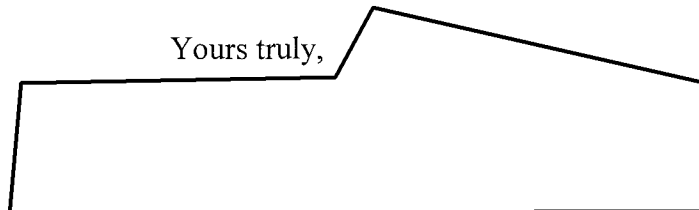
RE: Anonymous Romania

*ONE*

On 12 April 2012, the FBI received information that members of Anonymous in Romania hacked the website for the Romanian Minister of European Foreign Affairs, www.efinance.ro. The group responsible identifies themselves as "Malsec." The group has the following twitter account: @malsec.



Yours truly,



Federal Bureau of Investigation  
Legal Attache

By:   
Assistant Legal Attache

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.



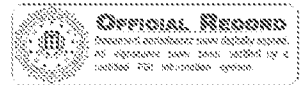
b3  
b7E

b7E

b6  
b7C

[REDACTED]

UNCLASSIFIED//~~FOUO~~



b3  
b7E

**FEDERAL BUREAU OF INVESTIGATION**  
**Import Form**

Form Type: EMAIL

Date: 07/09/2013

Title: (U//~~FOUO~~) CyWatch SitRep: Reported MALSEC Hacktivist Activity, [REDACTED]  
[REDACTED]

Approved By: UC [REDACTED]

Drafted By: [REDACTED]

Case ID #: [REDACTED]

Synopsis: (U//~~FOUO~~) CyWatch provided [REDACTED]  
[REDACTED] of reported hacktivist activity by MALSEC. CyWatch will continue to coordinate with trusted partners and pass information as it becomes available.

◆◆

b3  
b6  
b7C  
b7E

UNCLASSIFIED//~~FOUO~~

[REDACTED]

(U//~~FOUO~~) Based on current reporting, no further action is needed. However, CyWatch will share information with CyD as it becomes available.

Background:

(U//~~FOUO~~) USCYBERCOM reported this information to CyWatch [REDACTED]

CyWatch

[REDACTED]

Approved For Dissemination By:

SSA [REDACTED]

From: CYWATCH

b6  
b7C

Subject: CyWatch SitRep: MALSEC Hactivist activity reported by DC3

Categories:

Situation:

(U//~~FOUO~~) [redacted] Defense Cyber Crime Center / Defense Cyber Investigative Coordination Center (DC3 / DCISE) sent an email to the NTOC reporting MALSEC Hackers may have found links to

b7E

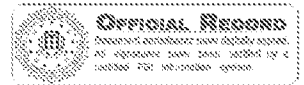
(U//~~FOUO~~) According to USCYBERCOM, the servers noted do not appear to have been compromised, but the attackers continue discussion of attempted access to [redacted]

Action:

b6  
b7C  
b7A  
b7E

[REDACTED]

UNCLASSIFIED//~~FOUO~~



b3  
b7E

**FEDERAL BUREAU OF INVESTIGATION**  
**Import Form**

**Form Type:** EMAIL

**Date:** 07/09/2013

**Title:** (U//~~FOUO~~) CyWatch SitRep Update 1: Reported MALSEC Hacktivist Activity, [REDACTED]

**Approved By:** UC [REDACTED]

**Drafted By:** [REDACTED]

**Case ID #:** [REDACTED]

**Synopsis:** (U//~~FOUO~~) CyWatch provided update [REDACTED] regarding reported MALSEC Hacktivist Activity. CyWatch will continue to coordinate with trusted partners and pass information as it becomes available.

◆◆

b3  
b6  
b7C  
b7E

UNCLASSIFIED//~~FOUO~~

Subject: CyWatch SitRep: MALSEC Hactivist activity reported by DC3

Situation:

(U//~~FOUO~~) [redacted] Defense Cyber Crime Center / Defense Cyber Investigative Coordination Center (DC3 / DCISE) sent an email to the NTOC reporting MALSEC Hackers may have found links to servers on [redacted]

b7E

(U//~~FOUO~~) According to USCYBERCOM, the servers noted do not appear to have been compromised, but the attackers continue discussion of attempted access to [redacted]

Action:

b6  
b7C  
b7A  
b7E

(U//~~FOUO~~) Based on current reporting, no further action is needed. However, CyWatch will share information with CyD as it becomes available.

Background:

(U//~~FOUO~~) USCYBERCOM reported this information to CyWatch [redacted]

CyWatch

b6  
b7C

Approved For Dissemination By:

SSA [redacted]

b7E

From: CYWATCH

[Redacted]

b6  
b7C

Subject: RE: CyWatch SitRep: MALSEC Hactivist activity reported by DC3

Categories:

[Redacted]

Please note that

[Redacted]

b7E

[Redacted]

CyWatch

[Redacted]

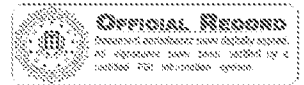
b6  
b7C

From: CYWATCH

[Redacted]

[Redacted]

b7E

UNCLASSIFIED//~~FOUO~~b3  
b7E**FEDERAL BUREAU OF INVESTIGATION**  
**Import Form****Form Type:** EMAIL**Date:** 07/22/2013**Title:** (U//~~FOUO~~) CyWatch SitRep: Reported CNA Activity by Hacktivist Group MALSEC, [REDACTED]**Approved By:** A/UC [REDACTED]**Drafted By:** [REDACTED]**Case ID #:** [REDACTED]

**Synopsis:** (U//~~FOUO~~) CyWatch provided notification [REDACTED]  
[REDACTED] of reported CNA Activity by the Hacktivist Group MALSEC. CyWatch will continue to coordinate with trusted partners and pass information as it becomes available.

◆◆

b3  
b6  
b7C  
b7EUNCLASSIFIED//~~FOUO~~



[REDACTED]

(U//~~FOUO~~) Based on current reporting, no further action is needed. However, CyWatch will share information with CyD as it becomes available.

Background:

(U//~~FOUO~~) USCYBERCOM reported this information to CyWatch [REDACTED]

CyWatch

[REDACTED]

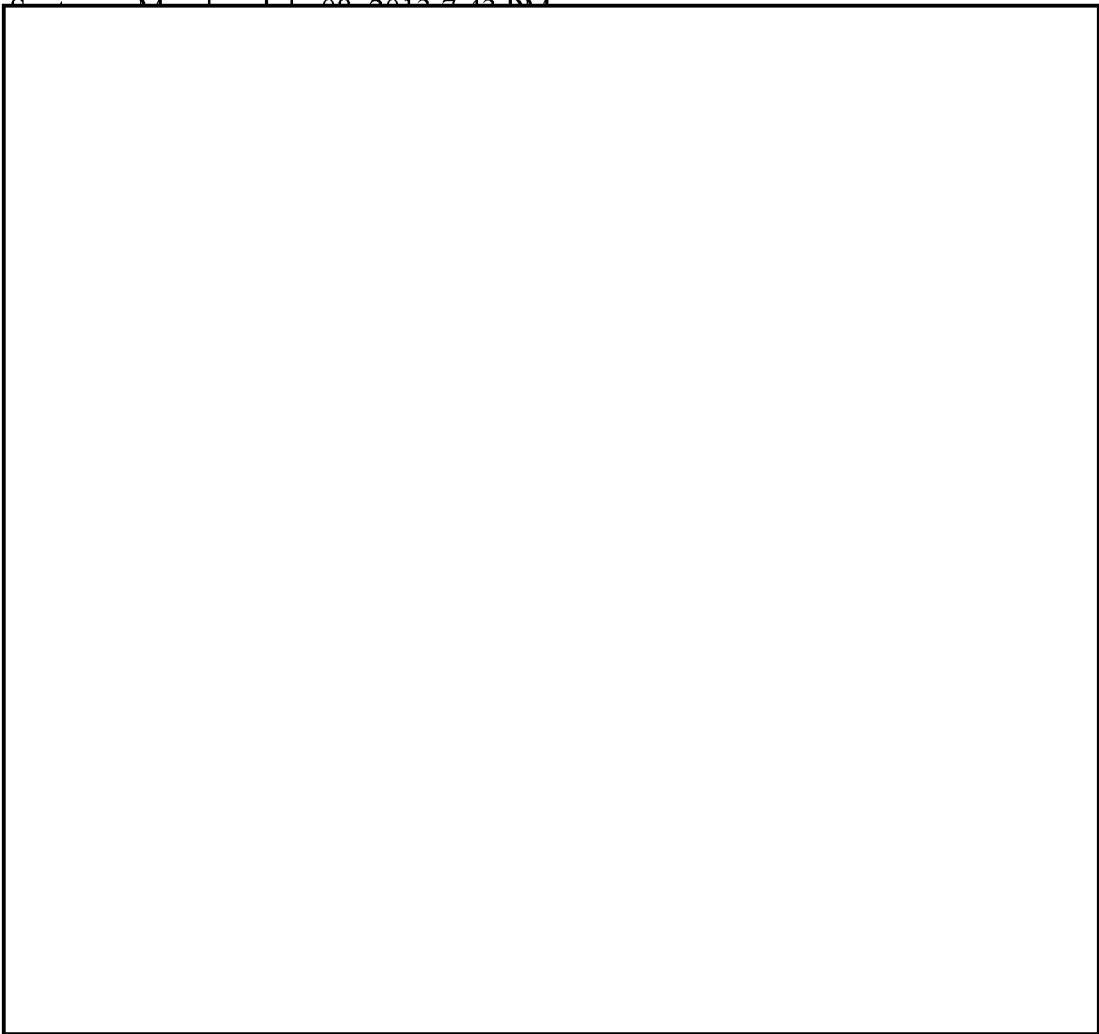
b6  
b7C

Approved For Dissemination By:

SSA [REDACTED]

From: CYWATCH

Sent: Monday, July 22, 2013 7:42 PM



b6  
b7C

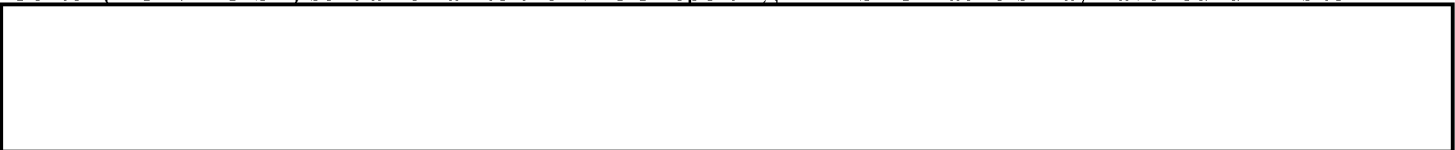
Subject: CyWatch SitRep: MALSEC Hactivist activity reported by DC3

Categories:



Situation:

(U//~~FOUO~~) [Redacted] Defense Cyber Crime Center / Defense Cyber Investigative Coordination Center (DC3 / DCISE) sent an email to the NTOC reporting MALSEC Hackers may have found links to



b7E

(U//~~FOUO~~) According to USCYBERCOM, the servers noted do not appear to have been compromised, but the attackers continue discussion of attempted access to [Redacted]

Action:



b6  
b7C  
b7A  
b7E



b7E

D  
egs

- 1 -

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/11/2012

[REDACTED]

b6  
b7C

[REDACTED] was interviewed on Friday, May 11, 2012 in Seattle, WA. After being advised of the identity of the interviewing Agent and the nature of the interview, [REDACTED] provided the following information:

[REDACTED]  
[REDACTED] met with Special Agents [REDACTED] in either 2010 or 2011 in response to a DDOS attack [REDACTED] initiated against the online moniker [REDACTED] stated

[REDACTED] MALICIOUS SECURITY (MALSEC), a splinter group of ANTISEC. This information was being furnished by [REDACTED]

MALSEC is [REDACTED] MALSEC operates from [REDACTED] and is believed to a safer alternative to [REDACTED] because users can connect using [REDACTED]

b6  
b7C  
b7EInvestigation on 5/11/2012 at Seattle, WAFile # [REDACTED] Date dictated n/aby [REDACTED]

132cjsd2

wpc  
b3  
b6  
b7C  
b7E

FEDERAL BUREAU OF INVESTIGATION  
FOI/PA  
DELETED PAGE INFORMATION SHEET  
FOI/PA# 1425666-0

Total Deleted Page(s) = 11  
Page 1 ~ b3; b6; b7A; b7C; b7E;  
Page 2 ~ b3; b6; b7A; b7C; b7E;  
Page 3 ~ b3; b6; b7A; b7C; b7E;  
Page 4 ~ b3; b6; b7A; b7C; b7E;  
Page 5 ~ b3; b6; b7A; b7C; b7E;  
Page 6 ~ b3; b6; b7A; b7C; b7E;  
Page 7 ~ b3; b6; b7A; b7C; b7E;  
Page 8 ~ b3; b6; b7A; b7C; b7E;  
Page 9 ~ b3; b6; b7A; b7C; b7E;  
Page 10 ~ b3; b6; b7A; b7C; b7E;  
Page 11 ~ b3; b6; b7A; b7C; b7E;

XXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
X Deleted Page(s) X  
X No Duplication Fee X  
X For this Page X  
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX